In the Office Action, Claims 1, 2, 5, 6, 7-9, 17, 18 and 21-25 were rejected under 35 U.S.C. §102(e) over U.S. Patent No. 6,018,724 to Arent.

Arent discloses a method for authenticating on-line transactions. The method is intended to address situations where a customer requests a proof of certification of a merchant. According to the Arent method, a certification authority must have pre-certified the merchant and provided the merchant with a digital certificate. In response to a customer's request for proof of certification, the Arent method contemplates that the merchant provides a digital certificate to the customer. The customer verifies the authenticity of the digital certificate with a software key which is publicly available. The software key may be unique to the customer. Upon verification, a certification indicator is visually displayed to the customer. For subsequent transactions, a merchant sends the same digital certificate to customer(s) and the customer(s) once again utilize the same software key for verification. Further, according to the Arent method, a plurality of merchants all utilize the same digital certificate and a plurality of customers repeatedly utilize the same, albeit unique, software keys for verification. The customer may customize their certification indicator with a text string. The customer selects the text string. The digital certificate, the software keys, and certification indicator, whether customized or not, are reused repeatedly. The text string which customizes the certification indicator is fixed, static and permanent. The text string is not used to perform the certification in order to establish a secure connection. Thus, if a merchant's digital certificate is stolen, the digital certificate will continue to function to improperly indicate secure access.

In contrast, Claim 1 recites a system including at least two parts or stations wherein a transaction or connection between any two or more of the parts or stations is conducted or established by means of an access code. The access code is available to an accessed part or station and requires an identical access code to be provided to an

accessing part or station at the time of conducting the transaction or establishing the connection. The access code is one of a plurality of codes provided to the accessed part or station and available to the accessing part or station. The access code is selected from the plurality of codes at the time of conducting the transaction or establishing the connection such that no two transactions are conducted or no two connections are established with the same access code. Consequently, each access code is unique, stored at two locations and only used once. Because every transaction uses a new and different access code, the security and reliability of the transaction and environment is significantly increased. As a result, the users code cannot be easily intercepted, stolen and improperly used because the access code is never the same. Arent does not disclose or suggest such a system configuration. Accordingly, Claim 1 and each of the claims depending therefrom distinguish the subject invention from Arent and, therefore, withdrawal of the rejection is respectfully requested.

With respect to Claim 17, a method of conducting a transaction or establishing a connection between at least two parts or stations by means of an access code is recited. The access code is available to an accessed part or station at the time of conducting the transaction or establishing the connection and requiring an identical access code to be provided to an accessing part or station. The method includes the steps of making available a plurality of codes to the accessed and the accessing parts or stations, selecting, at the time of conducting the transaction or establishing the connection, one code from the plurality of codes. The method further includes the steps of using the selected code to conduct the transaction or establish the connection such that no two transactions are conducted or no two connections are established with the same access code. Consequently, each access code is unique, stored at two locations and only used once. Arent does not disclose or suggest such a method. The presently claimed method thus provides enhanced security and reliability to transactional communications.

Accordingly, Claim 17 and each of the claims depending therefrom distinguish over Arent and, therefore, withdrawal of the rejection is respectfully requested.

In the Office Action, Claims 14, 16, 30, 32 and 35 were rejected under 35 U.S.C. §103(a) over U.S. Patent No. 6,018,724 to Arent in view of U.S. Patent No. 5,696,909 to Wallner.

As noted above, Arent discloses a merchant-provided digital certificate methodology in which the certificate is verified with a customer software key. The digital certificate and the software key are not the same. According to the Arent methodology, neither the digital certificate nor the software key are modified, varied or altered during repeated use.

Wallner discloses a virtual terminal for processing transactions.

With respect to Claims 14 and 16, it is respectfully submitted that Wallner does not overcome the deficiencies of Arent, as noted above with respect to Claim 1. In particular, neither Arent nor Wallner disclose or suggest, either alone or in combination, in whole or in part, a system including, *inter alia*, at least two stations wherein the access code is one of a plurality of codes provided to the accessed station and available to the accessing station, the access code being selected from the plurality of codes at the time of conducting the transaction such that no two transactions are conducted with the same access code as recited by Claim 1. Consequently, according to the presently claimed system, each access code is unique, stored at two locations and only used once. Accordingly, Claims 14 and 16 are not rendered obvious by the combination of references and withdrawal of the rejection under 35 U.S.C.§103(a) is respectfully requested.

With respect to Claims 30 and 32, it is respectfully submitted that Wallner does not overcome the deficiencies of Arent, as noted above with respect to Claim 17. In particular, neither Arent nor Wallner disclose or suggest, either alone or in combination,

in whole or in part, a method including, *inter alia*, the steps of conducting a transaction between at least two parts by means of an access code, the method including the steps of making available a plurality of codes to the accessed and the accessing parts or stations, selecting, at the time of conducting the transaction or establishing the connection, one code from the plurality of codes and using the selected code to conduct the transaction or establish the connection such that no two transactions are conducted or no two connections are established with the same access code as recited by Claim 17. Consequently, each access code is unique, stored at two locations and only used once. Accordingly, Claims 30 and 32 are not rendered obvious by the combination of references and withdrawal of the rejection under 35 U.S.C.§103(a) is respectfully requested.

With respect to Claim 35, it is respectfully submitted that the Examiner mischaracterizes what is disclosed by Arent. Column 4, lines 41-45 of Arent teach customizing a certification indicator. Such customized certification indicator is used repeatedly without variation thereafter. Wallner does not overcome this deficiency. In particular, neither Arent nor Wallner disclose or suggest, either alone or in combination, in whole or in part, a method of establishing secure connections between a provider and a customer including the steps of: providing a memory device for storing a first set of codes, wherein the memory device can receive, store and delete sets of codes which are accessible by the customer; storing a plurality of sets of codes with the provider, wherein the plurality of sets of codes includes the first set of codes; receiving a first customer code from the customer during establishing a secure connection, the first code being selected from the first set of codes stored on the memory device; accessing a first provider code from the first set of codes stored with the provider; comparing the first customer code with the first provider code, wherein a perfect match is a successful verification; establishing a secure connection to the customer when a successful

-6-

verification occurs; and preventing further use of the first customer code by the customer by deleting the first provider code. Consequently, two copies of the access codes exist, one at the customer and one at the provider. The customer does not generate the codes. However, the customer does transmit the codes to the provider to establish a secure connection. Accordingly, claim 35 is not rendered obvious by the combination of references and withdrawal of the rejection under 35 U.S.C. § 103(a) is respectfully requested.

In the Office Action, Claims 10 and 26 were rejected under 35 U.S.C. §103(a) over U.S. Patent No. 6,018,724 to Arent.

As noted above, Arent discloses a merchant-provided digital certificate which is verified with a customer software key. The digital certificate and the software key are not the same. Neither the digital certificate nor the software key are modified during repeated use. Thus, if a digital certificate is stolen, the theft of identity may be repeated over a period of time until the rightful owner discovers the theft and endeavors to cease the improper activity.

It is respectfully submitted that Arent does not disclose or suggest, in whole or in part, a system including, *inter alia*, at least two stations wherein a transaction between any two stations is conducted by means of an access code, the access code being available to an accessed station and requiring an identical access code to be provided to an accessing station at the time of conducting the transaction, wherein the access code is one of a plurality of codes provided to the accessed station and available to the accessing station, the access code being selected from the plurality of codes at the time of conducting the transaction such that no two transactions are conducted with the same access code as recited by Claim 1. Consequently, each access code is unique, stored at two locations and only used once for greater security. With such codes, if a code is stolen during use, the code cannot be reused. Accordingly, Claim 10 is not rendered

obvious by Arent and withdrawal of the rejection under 35 U.S.C.§103(a) is respectfully requested.

With respect to Claim 26, it is respectfully submitted that Arent does not disclose or suggest, in whole or in part, a method including the steps of conducting a transaction or establishing a connection between at least two parts or stations by means of an access code, the access code being available to an accessed part or station at the time of conducting the transaction or establishing the connection and requiring an identical access code to be provided to an accessing part or station, the method including the steps of making available a plurality of codes to the accessed and the accessing parts or stations, selecting, at the time of conducting the transaction or establishing the connection, one code from the plurality of codes and using the selected code to conduct the transaction or establish the connection such that no two transactions are conducted or no two connections are established with the same access code as recited by Claim 17. Consequently, each access code is unique, stored at two locations and only used once. Accordingly, Claim 26, at least by virtue of its dependency upon Claim 17, is not rendered obvious by the reference cited by the Examiner and withdrawal of the rejection under 35 U.S.C.§103(a) is respectfully requested.

In the Office Action, Claims 3, 4, 11-13, 15, 19, 20, 27-29 and 31 were rejected under 35 U.S.C. §103(a) over U.S. Patent No. 6,018,724 to Arent in view of U.S. Patent No. 4,630,201 to White.

As noted above, Arent discloses a merchant-provided digital certificate which is verified with a customer software key. The digital certificate and the software key are not the same. Neither the digital certificate nor the software key are modified, varied or altered during repeated use.

White discloses an on-line transaction security system having a portable transaction device 34 and a central processor 20. The transaction device 34 receives a

smart memory card to conduct a transaction. At the time of transaction, the transaction device 34 and the central processor 20 each generate a security code by algorithmically combining a transaction number (e.g., check number) and a random number. Upon generation of the security code, the transaction device 34 transmits its security code to the central processor 20 where it is compared with the security code generated by the central processor 20.

It is respectfully submitted that White does not overcome the deficiencies of Arent, as noted above with respect to Claim 1. In particular, neither Arent nor White disclose or suggest, either alone or in combination, in whole or in part, a system including, *inter alia*, at least two stations wherein a transaction between any two stations is conducted by means of an access code, the access code being available to an accessed station and requiring an identical access code to be provided to an accessing station at the time of conducting the transaction, wherein the access code is one of a plurality of codes provided to the accessed station and available to the accessing station, the access code being selected from the plurality of codes at the time of conducting the transaction such that no two transactions are conducted with the same access code as recited by Claim 1. Consequently, each access code is unique, only used once and stored at the two parts prior to the time of transaction. The codes of the subject claim are used directly without algorithmic calculation. No skipping of codes or additional apparatus to generate the codes is required. Thus, the use of codes directly is more efficient than that of the Arent and/or White methodology. Accordingly, Claims 3, 4, 11-13 and 15, at least by virtue of their dependency upon Claim 1, are not rendered obvious by the combination of references and withdrawal of the rejection under 35 U.S.C.§103(a) is respectfully requested.

With respect to Claims 19, 20, 27-29 and 31, it is respectfully submitted that White does not overcome the deficiencies of Arent, as noted above with respect to

Claim 17. In particular, neither Arent nor White disclose or suggest, either alone or in combination, in whole or in part, a method including the steps of conducting a transaction or establishing a connection between at least two parts by an access code is recited. The access code is available to an accessed part or station at the time of conducting the transaction or establishing the connection and requiring an identical access code to be provided to an accessing part. The method further includes the steps of making available a plurality of codes to the accessed and the accessing parts, selecting, at the time of conducting the transaction or establishing the connection, one code from the plurality of codes and using the selected code to conduct the transaction or establish the connection such that no two transactions are conducted or no two connections are established with the same access code as recited by Claim 17. Consequently, each access code is unique, stored at two locations prior to the time of transaction and only used once. The codes of the subject claim are used directly without algorithmic calculation. Thus, the use of mere selection of codes at the time of transaction is more efficient than that of the Arent and/or White methodology. Accordingly, Claims 19, 20, 27-29 and 31, at least by virtue of their dependency upon Claim 17, are not rendered obvious by the combination of references and withdrawal of the rejection under 35 U.S.C.§103(a) is respectfully requested.
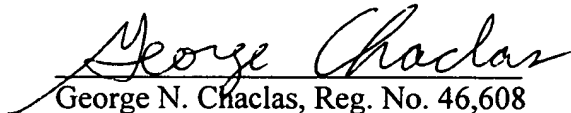
Applicant's representative has added new Claim 36 which is directed to additional patentable aspects of the subject invention. Applicant's representative respectfully submits that new Claim 36 patentably distinguishes over the art of record, and allowance is respectfully requested.

Any additional fees or overpayments due as a result of filing the present paper may be applied to Deposit Account No. 50-1631. It is respectfully submitted that all of the claims now remaining in this application, namely Claims 1-32, 35 and 36, are in condition for allowance, and such action is earnestly solicited.

If after reviewing this Amendment, the Examiner believes that a telephone interview would facilitate the resolution of any remaining matters the undersigned attorney may be contacted at the number set forth hereinbelow.

Respectfully submitted,

Date : December 27, 2001

George N. Chaclas, Reg. No. 46,608
Cummings & Lockwood
Attorney for Applicant
CityPlace I
185 Asylum Street
Hartford, CT 06103
Tel: (860) 275-7045

.HrtLib1:381894.1 12/27/01

-11-